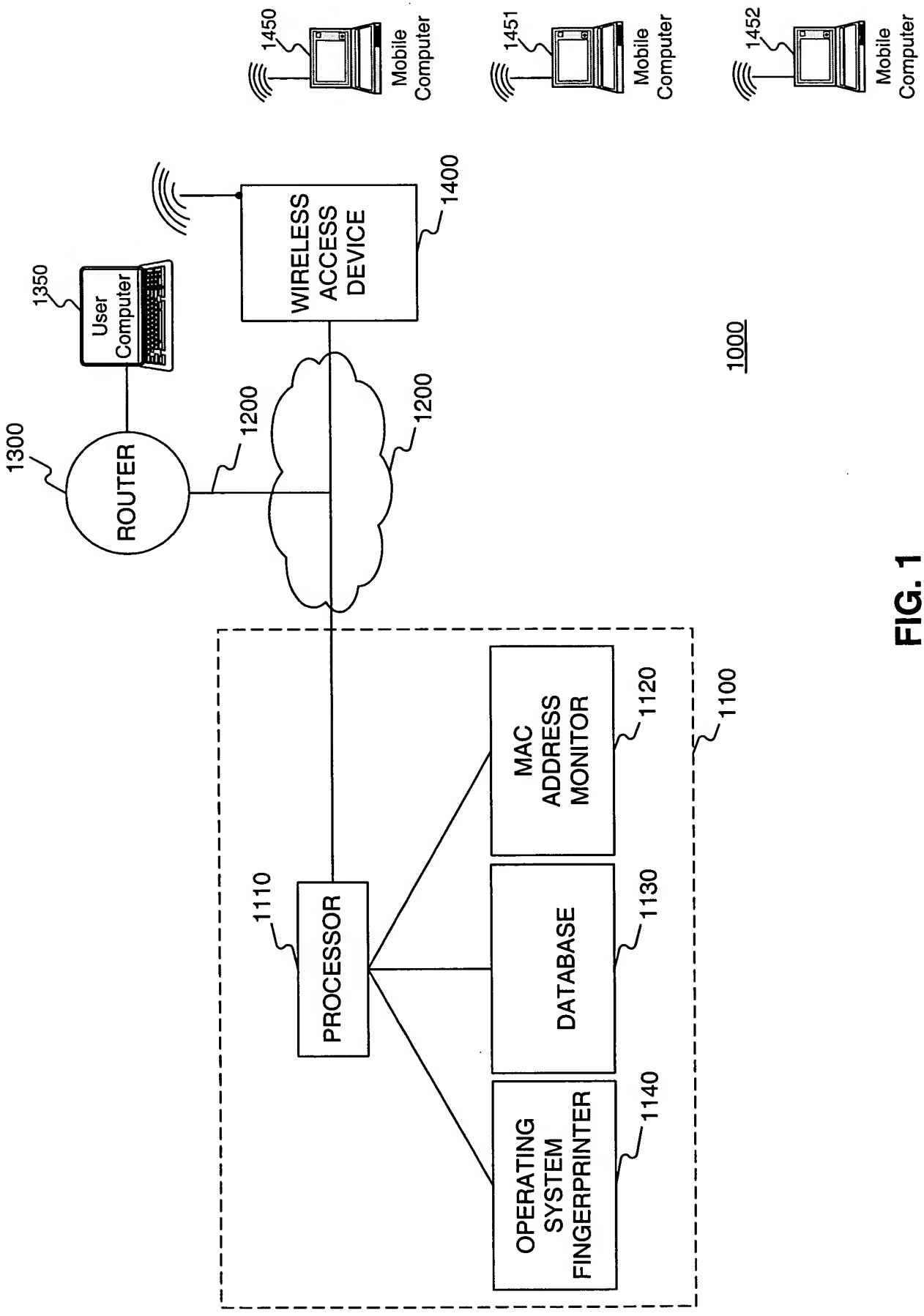
1450
Mobile Computer
1451
Mobile Computer
1452
Mobile Computer
WIRELESS ACCESS DEVICE
1400
1350
User Computer
1300
ROUTER
1200
1200
1000
1110
PROCESSOR
MAC ADDRESS MONITOR
1120
DATABASE
1130
OPERATING SYSTEM FINGERPRINTER
1140
1100

FIG. 1

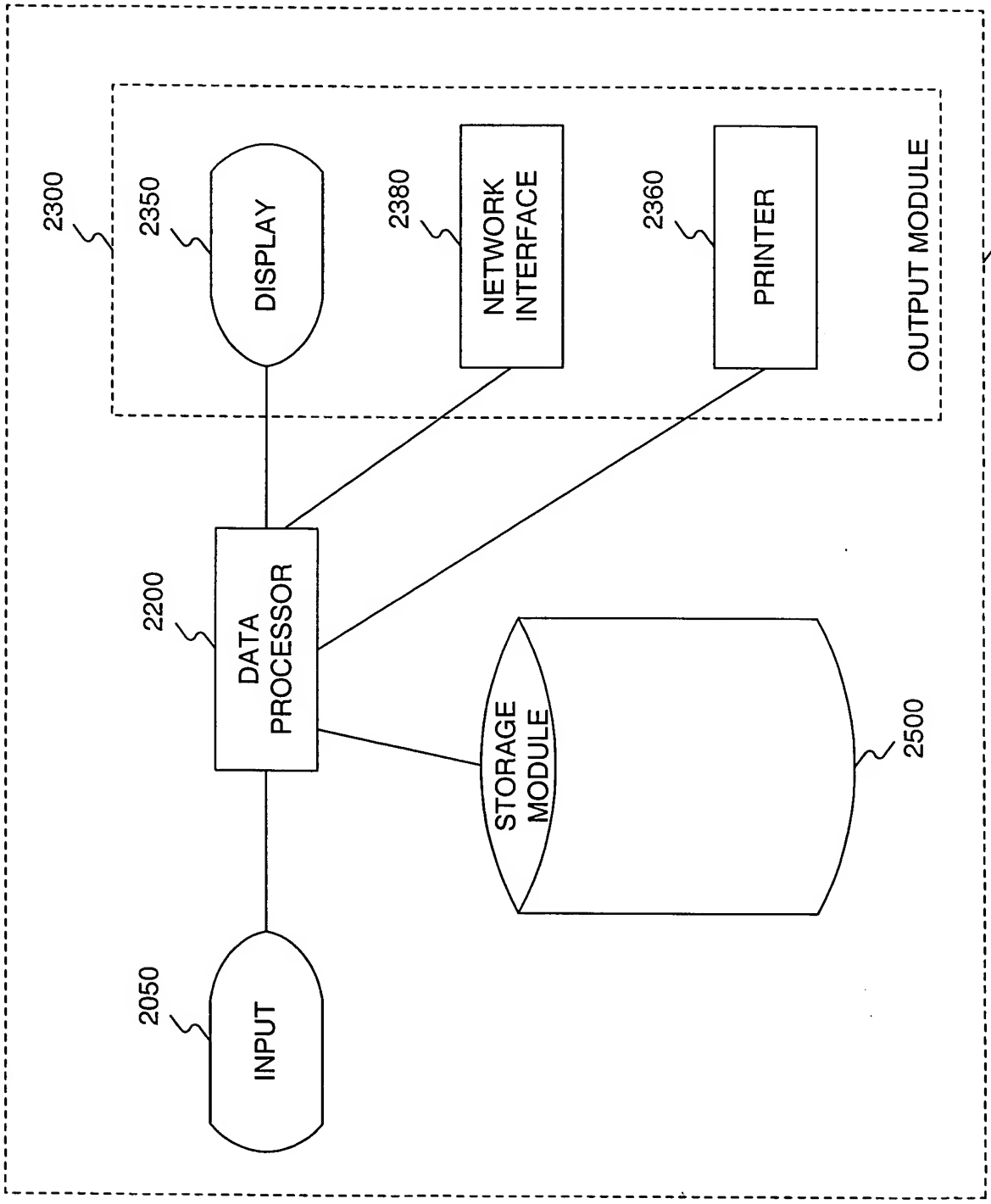
2300
2350
DISPLAY
2380
NETWORK INTERFACE
2360
PRINTER
OUTPUT MODULE
2000
2200
DATA PROCESSOR
STORAGE MODULE
2500
2050
INPUT

FIG. 2

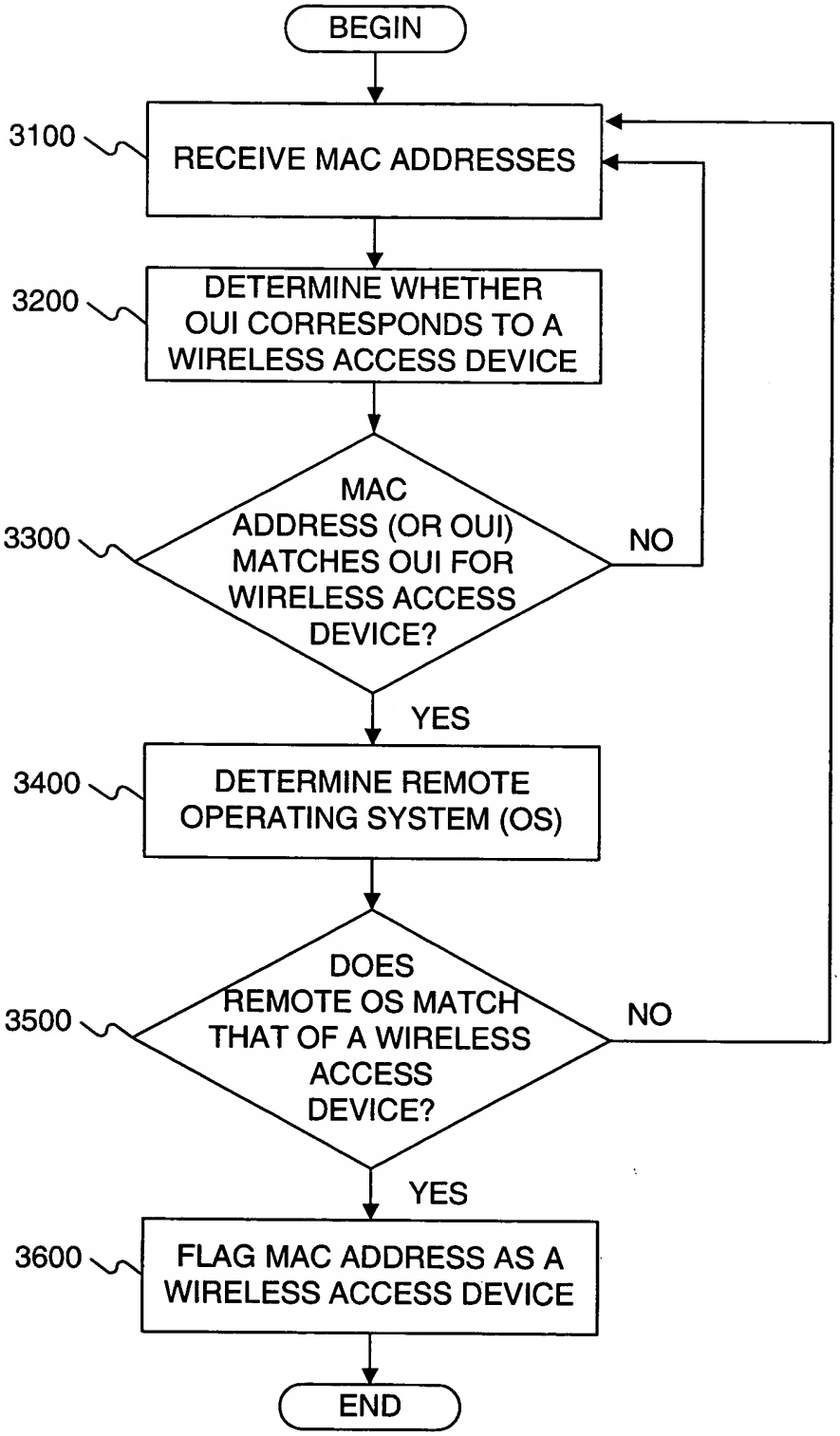
BEGIN
3100
RECEIVE MAC ADDRESSES
3200
DETERMINE WHETHER OUI CORRESPONDS TO A WIRELESS ACCESS DEVICE
3300
MAC ADDRESS (OR OUI) MATCHES OUI FOR WIRELESS ACCESS DEVICE?
NO
YES
3400
DETERMINE REMOTE OPERATING SYSTEM (OS)
3500
DOES REMOTE OS MATCH THAT OF A WIRELESS ACCESS DEVICE?
NO
YES
3600
FLAG MAC ADDRESS AS A WIRELESS ACCESS DEVICE
END

FIG. 3

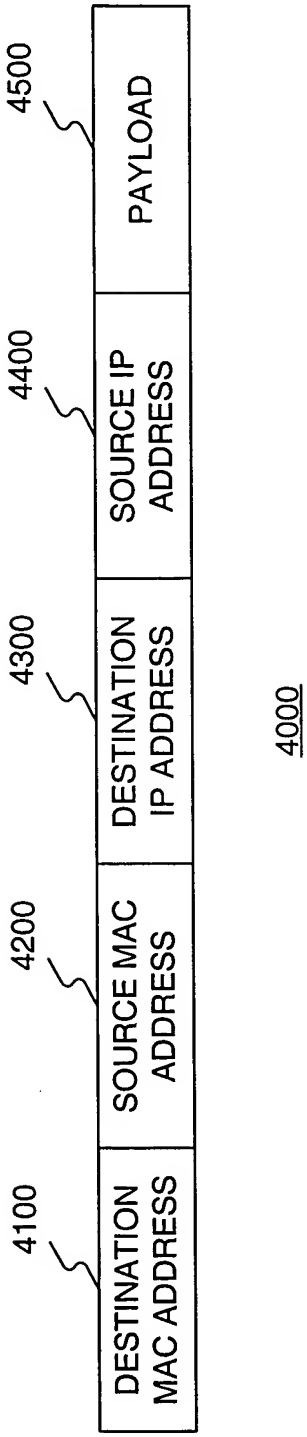
4500
PAYLOAD
4400
SOURCE IP ADDRESS
4300
DESTINATION IP ADDRESS
4200
SOURCE MAC ADDRESS
4100
DESTINATION MAC ADDRESS
4000

FIG. 4

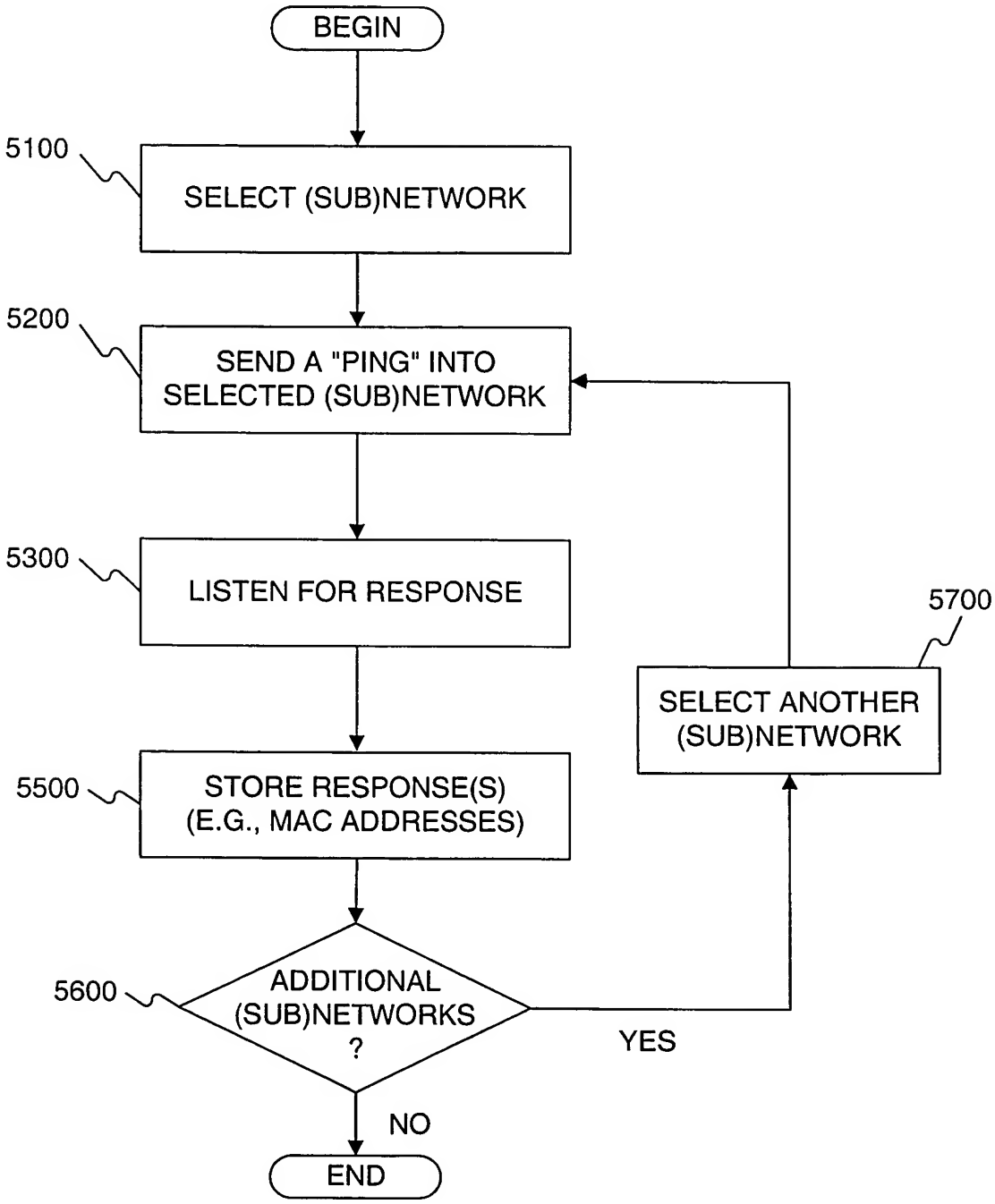
BEGIN
5100
SELECT (SUB)NETWORK
5200
SEND A "PING" INTO
SELECTED (SUB)NETWORK
5300
LISTEN FOR RESPONSE
5500
STORE RESPONSE(S)
(E.G., MAC ADDRESSES)
5600
ADDITIONAL
(SUB)NETWORKS
?
YES
NO
5700
SELECT ANOTHER
(SUB)NETWORK
END

FIG. 5

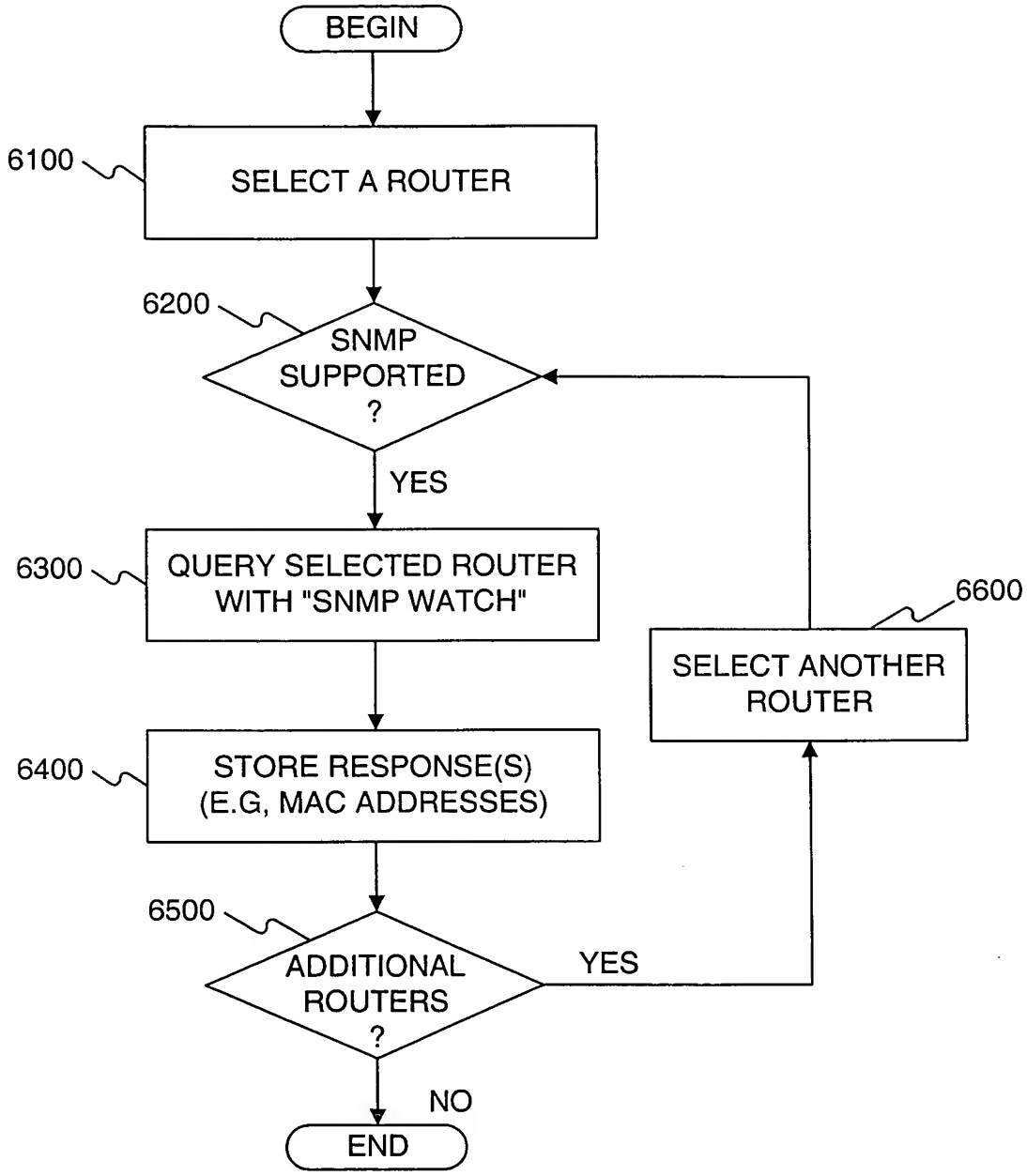
BEGIN
6100
SELECT A ROUTER
6200
SNMP SUPPORTED ?
YES
6300
QUERY SELECTED ROUTER WITH "SNMP WATCH"
6400
STORE RESPONSE(S) (E.G, MAC ADDRESSES)
6500
ADDITIONAL ROUTERS ?
YES
NO
END
6600
SELECT ANOTHER ROUTER

FIG. 6

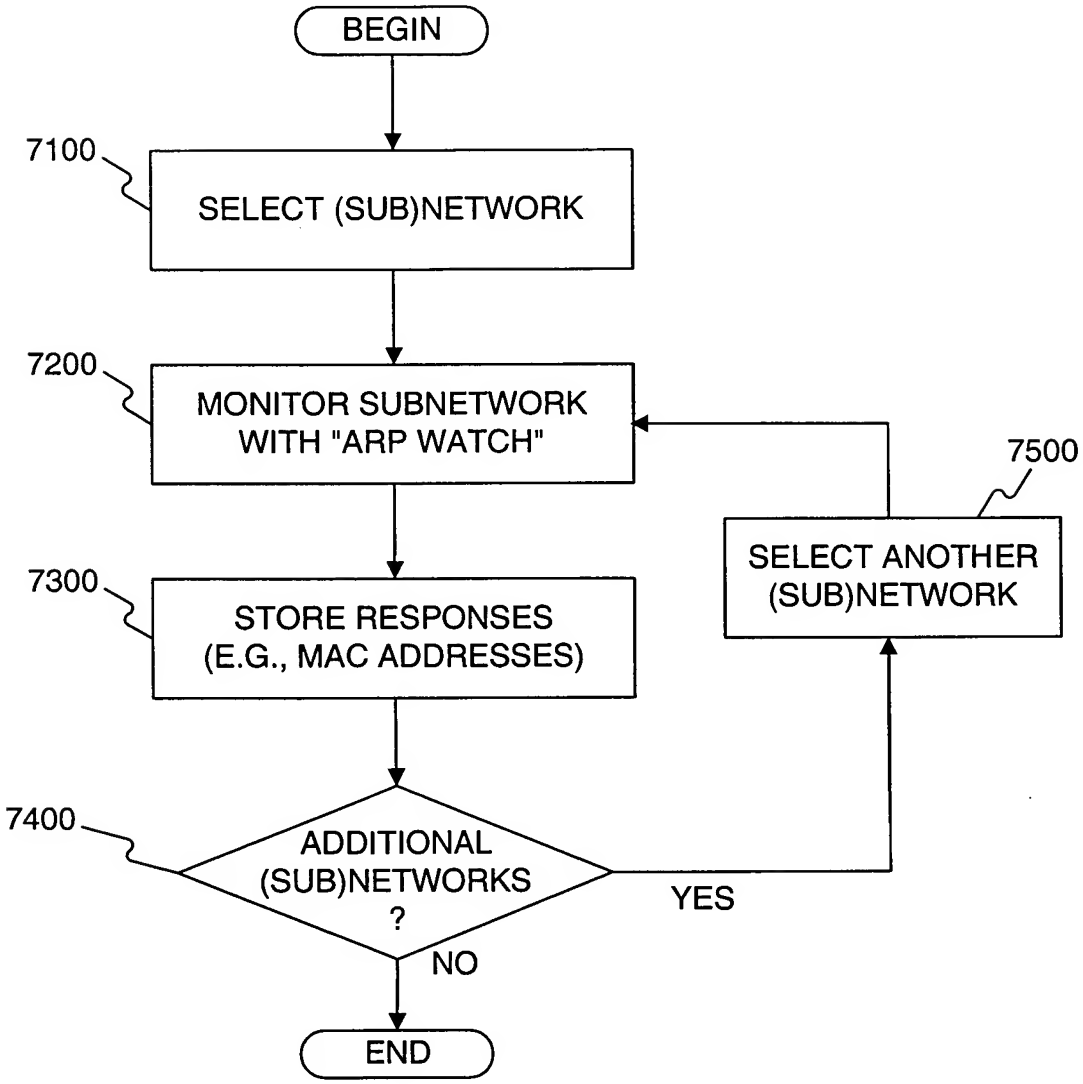
BEGIN
7100
SELECT (SUB)NETWORK
7200
MONITOR SUBNETWORK WITH "ARP WATCH"
7300
STORE RESPONSES (E.G., MAC ADDRESSES)
7400
ADDITIONAL (SUB)NETWORKS ?
YES
NO
7500
SELECT ANOTHER (SUB)NETWORK
END

FIG. 7

```
From: arpwatch@host1.test.com (Arpwatch)
To: root@host1.test.com
Subject: new station (ap.test.com)

        hostname: ap.test.com          8200
      ip address: 10.0.0.1
 ethernet address: 0:2:2d:68:a:88      8100
8300 ethernet vendor: Agere Systems
      timestamp: Tuesday, April 15, 2003 10:58:13 -0400
```

8000

FIG. 8